Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Cyber Threats to Healthcare Technology Services: a Case Study

Rodrigo Sousa

Universidade Lusófona - CUP, Porto, Portugal
Email: rodrigosousa1105@gmail.com

Abstract

Information Technology has become a key component of many sectors in today's world, and healthcare is a prime example. However, the increase in IT, particularly among healthcare businesses which are now identified as a major target area, has increased sensitivity to cyber threats. There is a variety of vital data stored in such facilities, including private and possibly financial information about patients. An analysis of the risks and threats to these institutions is presented in this paper. The study is based on the results of a survey involving several healthcare professionals from various healthcare establishments in Portugal. It aims to draw attention to the current state of healthcare cybersecurity and evaluate its possible risks, as well as how best to mitigate them. This in-depth analysis, aiming at contributing significantly to the conversation on the cybersecurity of healthcare and eventually improving patient data security and integrity against increasing cyber threats, would be a major step forward.

Keywords: Cybersecurity; Healthcare; Cybercrime; Cyber Threats; Data Integrity; Threat Analysis

Citation: R. Sousa, "Cyber Threats to Healthcare Technology Services: A Case Study", *ARIS2-Journal*, vol. 4, no. 1, pp. 35–46, Apr. 2024.

DOI: https://doi.org/10.56394/aris2.v4i1.38

* Corresponding author. Email address: rodrigosousa1105@gmail.com

1. Introduction

We live in a world where healthcare institutions have more to worry about than just providing medical services to people. With the advancement of technology in recent decades cybersecurity and patient data protection have become some of the most significant concerns. Healthcare technology ranges from those that store electronic health records (EHRs), those that monitor health and dispense medicines (general purpose devices and wearables, as well as technology embedded in the human body), to telemedicine technology that delivers treatment remotely to any part of the world [1]. Healthcare has advanced a lot with this information and communication technology (ICT) adoption, and we can see it everywhere, like our phones that now can have mobile apps with services such as appointment booking, digital medical analysis reports, online payment, digital medical prescriptions, etc., that allow the patient not to have to go to the institution in person like in the past [2]. However, this massive digitalization has not only brought good things, it has also increased the attack surface of these institutions. With all this connectivity between devices, hackers now have more open routes. When it comes to hospitals, cyber-attacks can have disastrous consequences, as demonstrated by the tragic incident that occurred in September 2020 in Germany. A 78-year-old woman who had suffered an aneurysm died on her way to the hospital, which was twenty kilometers away, due to a ransomware attack on the University Hospital of Düsseldorf. This attack caused network failures, resulting in the emergency department's closure and the police considering the death as a homicide by negligence. The hackers were contacted to provide the digital key to decrypt the hospital's 30 encrypted servers. However, despite knowing that their target victim was a hospital, the hackers were unaware that the emergency department server was among the encrypted ones. This incident may have been the first known instance of a ransomware attack resulting in a deadly victim [3].

In addition to the need for the implementation of strong cybersecurity measures and modern technology, the institutions have something else to worry about that is the human component which remains a key weakness that hackers may exploit through Social Engineering [4]. Digital systems and data security can be compromised by men errors such as choosing weak passwords, falling for Phishing attacks, or failing to comply with security protocols, these acts could allow hackers to penetrate them. This emphasizes the crucial role of human error in data breaches, which according to the 2023 Verizon Data Breach Investigations Report accounted for around 74% of incidents, being the three primary ways in which attackers access an organization, stolen credentials, phishing, and exploitation of vulnerabilities [5]. Section 2 of this paper talks about the main cybersecurity concerns in the healthcare sector and why it is an attractive target for cybercriminals. Section 3 categorized the main types of cyber threats faced by the healthcare industry. Each of these threats has been described in detail, highlighting how they can impact healthcare institutions and patients. In the fourth section, there is a case study where a survey was made to health professionals to understand the current state of cybersecurity in these institutions and their level of knowledge. Finally, in section 5 we draw the conclusions.

2. Healthcare vulnerabilities and why it is targeted

In the past, it was believed that nobody would want to attack health care systems and protective measures were not considered necessary, the institutions were focused on providing medical care [1]. However, more and more institutions are realizing what a serious problem it can be not to be well prepared against cyber-attacks. The

cybersecurity of healthcare services can be divided into a number of aspects, ranging from the protection of patient's personal data to also safeguarding hospital funds and allowing control and secure access to medical information as well as ensuring that health devices operate at their optimum performance when they are required [3]. There are several problems that have increased vulnerability in health institutions:

- Increasingly connected technology allows better care for patients, particularly when they are suffering from chronic illnesses [6]. This allows for multiple connections to medical devices [7]. Devices are frequently easily accessible, increasing the risk that an attacker will find them. A single device can allow an access point on a larger hospital network, bypassing firewalls. The gap between attacks and identification of breaches also contributes to an increased risk.
- Increased focus on patient health, which will lead to more continuous patient monitoring outside the institutional environment [8]. The use of more devices in healthcare settings increases the risk of security breaches.
- Widespread adoption of mobile consumer devices, such as smartphones, makes it difficult to protect health data from risks posed by general-purpose devices [6].

Despite this growth in new technologies, many healthcare institutions continue to rely on legacy systems like as operating systems. Microsoft has not supported Windows XP since 2014, making it easier for hackers and viruses to go undetected [9]. Insufficient funding for cybersecurity is also a source of worry. While organizations invest in integration, they do not prioritize software and security system upkeep. This problem is exacerbated by the industry's lack of cybersecurity skill, which is linked to the high cost of cybersecurity experts and a general lack of technological experience [1]. Healthcare is a prime target for cyberattacks due to the potential for significant financial and political gain. It is attractive for financial exploitation, including identity theft, insurance fraud or even organized crime activities due to the high value of medical data which may exceed $1,000 on a full set of medical credentials [1]. Stolen medical identities can be used to obtain health services and prescription medication by assuming someone's identity or insurance credentials. Sometimes there is even sufficient information in medical records to open bank accounts, secure loans or obtain passports [10]. Political value is also a factor, as seen in the attack on the World Anti-Doping Agency where athletes' records were made public [11]. Healthcare websites, accessed by millions, can be used for propaganda, as evidenced by the hacking of the United Kingdom National Health Service (NHS) websites when cyberterrorists uploaded images of Syrian civil war [12]. Cybersecurity enthusiasts also target healthcare systems to expose security vulnerabilities, as seen in the 2016 incident involving the Australian Blood Donor service, where more than half a million of prospective blood donors had their personal information exposed [13]. In summary, the healthcare sector's shift to digital platforms and devices, coupled with insufficient cybersecurity measures and understanding of staff behaviors, has made it a prime target for cyberattacks. These attacks aim for financial or political gain, or to expose vulnerabilities.

3. Cyber threats to healthcare

Simply establishing a cybersecurity department and investing money to improve corporate cybersecurity measures is inadequate. Collaboration across many sectors in the cybersecurity business, as well as a proactive attitude to developing solutions for more complex cyber-attacks, are critical. Nonetheless, attacks against healthcare

institutions can be categorized into five groups based on the system vulnerabilities exploited, the potential consequences, and the defensive strategies employed [14][15].

3.1. Social engineering

The most common type of social engineering attack is Phishing and is one of the most common type of attacks in the healthcare sector too. These attacks often involve malicious links or attachments in widely distributed emails or text messages, which introduce malware into the organization [21]. The goal here is to steal personal or confidential data like credentials, which can be used for various types of fraud. The most common type of fraud is identity theft, where personally identifiable information is used to impersonate an individual [16]. Institutions that fall victim to phishing attacks may suffer reputational damage and incur additional expenses, such as penalties for unauthorized access to medical and patient data.

3.2. Ransomware

Ransomware is a malicious software that employs extortion tactics to target its victims. The attacker holds the victim's data hostage by encrypting it, making it inaccessible to the victim unless a ransom is paid [17]. In case the victim fails to pay the ransom, the attacker either discloses the data publicly or destroys it. Ransomware attacks can be devastating, particularly for businesses and organizations. Data is often the lifeblood of modern businesses, and losing access to critical data can result in significant financial losses, not to mention damage to the organization's reputation [22].

3.3. DoS and DDoS

A Denial of Service (DoS) attack seeks to stop or hobble access to services or data on the target machine. This can be accomplished by flooding the target with traffic or requests, thereby shutting down services [18]. This sort of attack can range from being just inconvenient, as in the instance of a Vandal attempting to disgrace a victim, to being life-threatening, if the service taken off is crucial to life support. A DoS attack is an example of ransomware. A Distributed Denial of Service (DDoS) attack, on the other hand, has the same purpose but is carried out in a more complicated method. Instead of a single infected system transmitting traffic or requests to a target, a DDoS assault leverages several compromised machines (often forming a botnet) to attack the target. DDoS attacks are more difficult to fight against since the attack traffic originates from a variety of sources, making it harder to prevent or filter [19].

3.4. Insider threats

Insider threats both unintentional and malicious, exist in every organization where employees have access to the IT system or parts of it. Accidental attacks are triggered by unintended information sharing or errors made by health professional. On the other hand, malicious attacks are performed by insiders seeking personal benefit, mostly financial or harm to the institution. Personal data, for example, might be duplicated and sold on the dark web by an employee with access to patient information [20]. Insider attacks, whether immediate or long-term, can have serious consequences for patients and healthcare institutions alike.

3.5. Lost and theft of equipment's

The theft of portable devices is a common occurrence, and if hackers gain access to these devices, such as doctors' laptops working remotely, they can cause significant harm to the institutions and patients. The loss of sensitive patient data can lead to a large-scale loss that directly damages the reputation of the doctor and the organization, and can lead to the identity theft of patients. In 2019, 572 security incidents were reported and a total of 41.1 million patient records were stolen [14].

4. Case study

This study was based on a survey of healthcare professionals from various institutions and aimed to understand the current state of cybersecurity in these institutions and their level of knowledge. The survey obtained a total of 161 responses from healthcare professionals from various healthcare institutions in Portugal and from various professional positions. Of these 161 participants, 27.3% (44 out of 161) are doctors, 43.5% (70 out of 161) are nurses, 28% (45 out of 161) are healthcare assistants, 0.6% (1 out of 161) are social assistants and 0.6% (1 out of 161) work in administration. Another piece of information about these people was their years of experience in the area: 29.8% (48 out of 161) have been working in the area for 5 years or less, 17.4% (28 out of 161) have between 5 and 10 years, 16.1% (26 out of 161) have between 10 and 15 years, 18% (29 out of 161) have between 15 and 20 years and 18.7% (30 out of 161) have more than 20 years' experience working as a health professional.

The first question asked was intended to find out whether or not professionals think they have any knowledge of cybersecurity, resulting in the circular graph in figure 1.

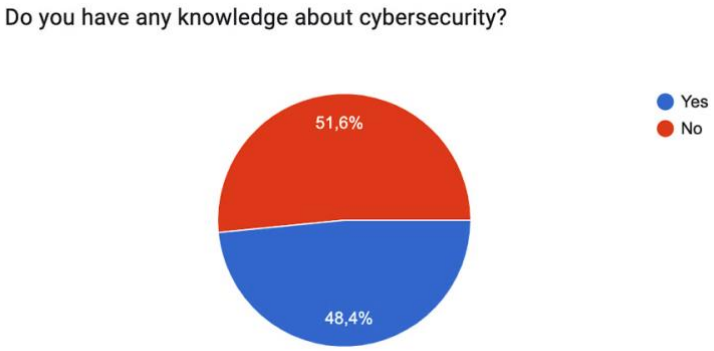

Figure 1: Pie chart of the results of the question: "Do you have any knowledge about cybersecurity?"

Looking at this graph, we can see that 51.6% (83 out of 161) of people admit to having no knowledge of cybersecurity, while 48.4% (78 out of 161) say they have some knowledge of cybersecurity.

Social engineering is a powerful tool and people must be prepared against it, so the questions on the area then began by asking people to indicate the correct definition of phishing which is one of the most frequent attacks:

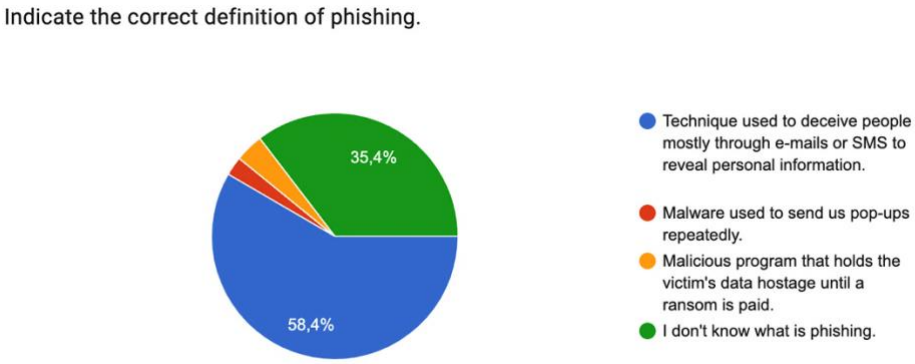

Figure 2: Pie chart of the results of the question: "Indicate the correct definition of phishing."

In this graph we can see that the majority of people, 58.4% (94 out of 161) know what phishing is, but even so, 35.4% (57 out of 161) don't know the term and 6.2% (10 out of 161) got the answer wrong. This represents a danger and is already the first indicator of a lack of preparation in cybersecurity. When asked if they had ever received an email or message that they suspected was a phishing attack, 39.1% (63 out of 161) of people said they had, 44.1% (71 out of 161) didn't know if they had or not and only 16.8% (27 out of 161) said they had never received one. When asked if they had ever received an email or message that they suspected was a phishing attack, 39.1% (63 out of 161) of people said they had, 44.1% (71 out of 161) didn't know if they had or not and only 16.8% (27 out of 161) said they had never received one.

Figure 3: Pie chart of the results of the question: "Have you received an email or message that you suspect was a phishing attack?"

Of the people who answered "Yes", 66.7% (42 out of 63) said they had reported the email/message and deleted or not opened any links, which is good and shows some kind of awareness and concern. The fourth question asked whether people knew what ransomware was, which is not a term that is well known to the average citizen, as reflected in the following graph, but it is one of the main threats to healthcare. In the graph we can see that 69.6% (112 out of 161) of people admit that they don't know what ransomware is, 13% (21 out of 161) got the answer

wrong, showing that they don't know either, and only 17.4% (28 out of 161) got the correct answer, "Malicious program that holds the victim's data hostage until a ransom is paid".

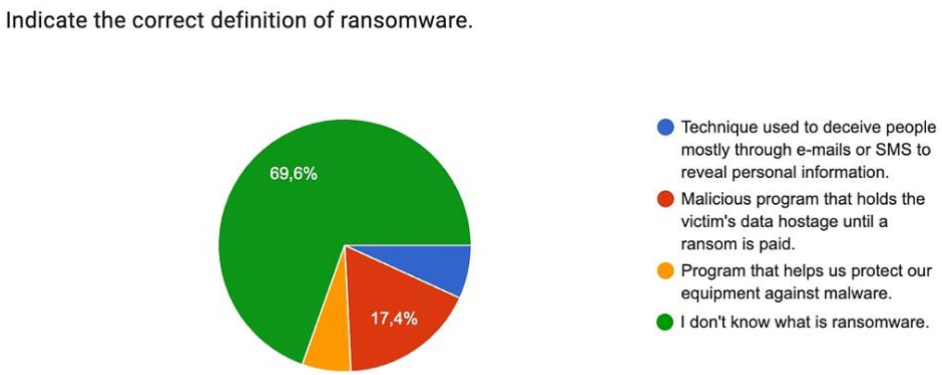

Figure 4: Pie chart of the results of the question: "Indicate the correct definition of ransomware."

Health professionals were asked if they access Wi-Fi in public places, to which 83.2% (134 out of 161) answered yes and 16.8% (27 out of 161) answered no. This bad habit can be a gateway to malicious software and this possibility will be exacerbated by the following responses to the survey.

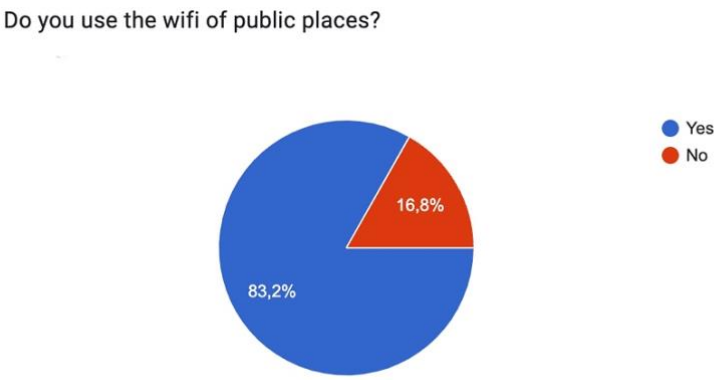

Figure 5: Pie chart of the results of the question: "Do you use the Wi-Fi of public places?"

The next question asked whether workers knew what a VPN was for, with 60.2% (97 out of 161) answering "Yes" and 39.8% (64 out of 161) answering "No", we can conclude that most people are familiar with the technology.

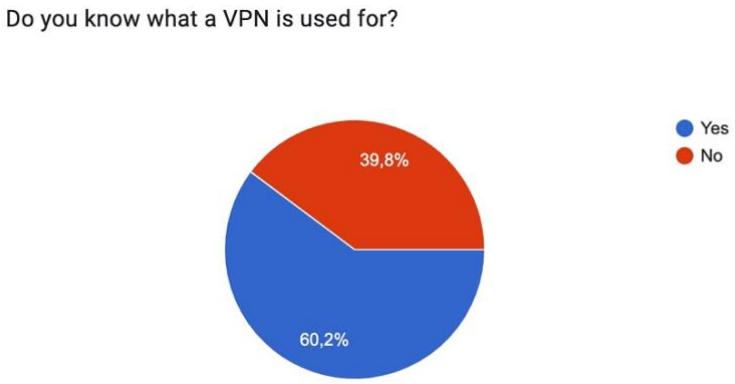

Figure 6: Pie chart of the results of the question: “Do you know what a VPN is used for?"

Although a lot of people know what a VPN is for, only 8.7% (14 out of 161) use one regularly, compared to an overwhelming majority of 91.3% (147 out of 161) who don't use it regularly, as we can see in figure 7.

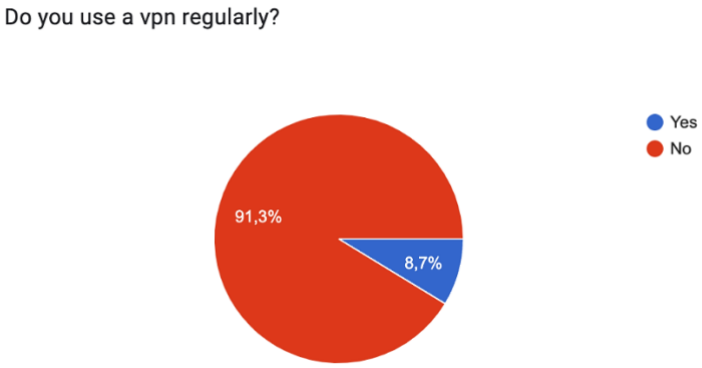

Figure 7: Pie chart of the results of the question: "Do you use a VPN regularly?"

When asked if they use their workplace Wi-Fi on their personal devices, 76.4% (123 out of 161) said that they do, while 23.6% (38 out of 161) do not. This combined with not using VPNs when accessing public Wi-Fi can be a gateway for a hacker into the institution's network.

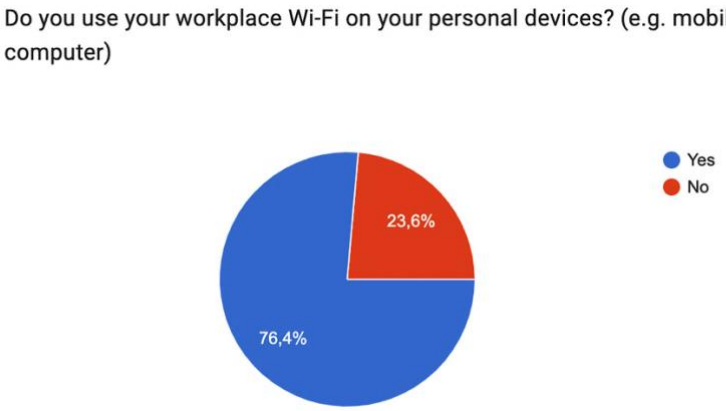

Figure 8: Pie chart of the results of the question: "Do you use your workplace Wi-Fi on your personal devices?"

The next question was about the software updates of the institutions, 38.5% (62 out of 161) of people said they rarely notice updates to the systems they use in their workplace, 34.8% (56 out of 161) notice updates sometimes, 9.3% (15 out of 161) notice updates frequently and 17.4% (28 out of 161) never notice updates. As discussed earlier in this paper, outdated systems are a major vulnerability for healthcare institutions.

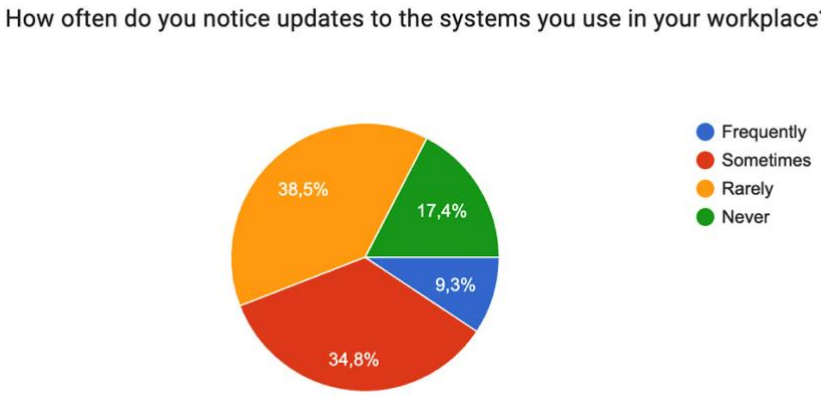

Figure 9: Pie chart of the results of the question: "How often do you notice updates to the systems you use in your workplace?"

It was also asked about the existence of protocols to report suspected computer security breaches in institutions. To which 85.1% (137 out of 161) of people answered "No" and 14.9% (24 out of 161) answered "Yes". This shows a lack of concern on the part of the institutions.

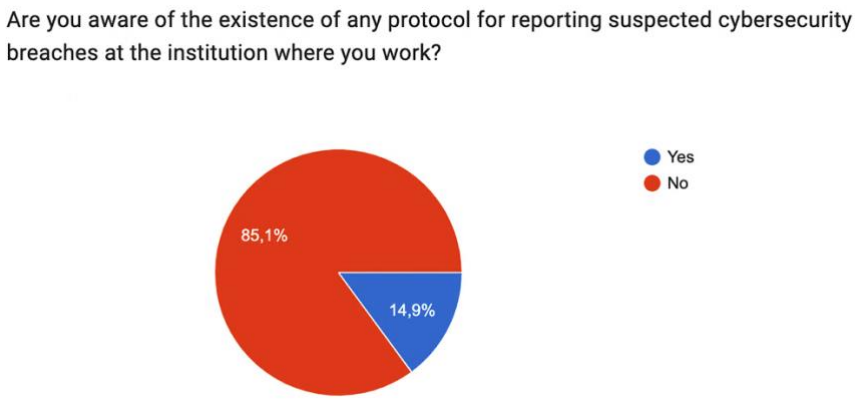

Figure 10: Pie chart of the results of the question: "Are you aware of the existence of any protocol for reporting suspected cybersecurity breaches at the institution where you work?"

Finally, healthcare professionals were asked if they think they are properly educated in cybersecurity, to which 92.5% (149 out of 161) answered yes. Concluding that they themselves perceive the lack of training in the area, which should be offered by the institutions.

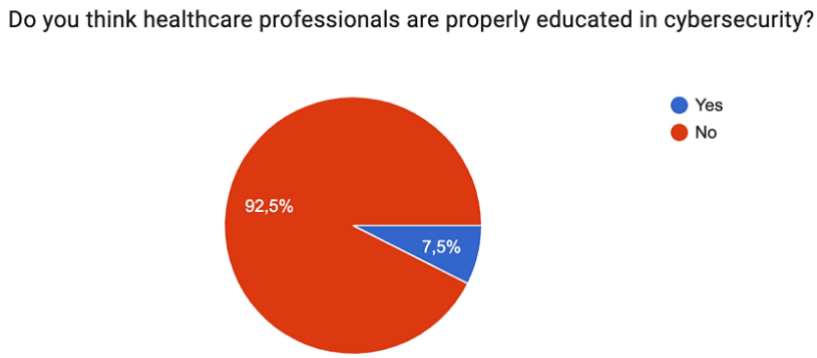

Figure 11: Pie chart of the results of the question: "Do you think healthcare professionals are properly educated in cybersecurity?"

5. Conclusions

Based on this case study, we can conclude that health professionals lack preparation and information about cybersecurity. The vast majority understand this lack of education and we can see this from the last survey question. This highlights the immediate need for institutions to provide extensive training and education to their staff regarding cybersecurity. It is important to emphasize the significance of protecting patient data and securing healthcare systems. In summary, this study emphasizes the need for strong cybersecurity measures, training, and institutional protocols within healthcare settings. Addressing these gaps is essential to strengthen defenses against cyber threats, protect patient information, and ensure the integrity and security of healthcare systems.

References

[1] Lynne Coventry, Dawn Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”, (2018), Available: https://doi.org/10.1016/j.maturitas.2018.04.008

[2] S. Sarowa, B. Bhanot, V. Kumar and M. Kumar, "Analysis of Attack Patterns and Cyber Threats in Healthcare Sector", 2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT), Dehradun, India, 2023, pp. 160-165, doi: 10.1109/DICCT56244.2023.10110141.

[3] Anthony Minnaar, Friedo JW Herbig, "Cyberattacks and the Cybercrime Threat of Ran-somware to Hospitals and Healthcare Services During the COVID-19 Pandemic", 2021, Available: https://hdl.handle.net/10520/ejc-crim_v34_n3_a10

[4] M. A. Fauzi, P. Yeng and B. Yang, "Correlating Healthcare Staff’s Stress Level and Cybersecurity Practices in Norway," 2023 Intelligent Methods, Systems, and Applications (IMSA), Giza, Egypt, 2023, pp. 235-240, doi: 10.1109/IMSA58542.2023.10217783.

[5] Verizon, “2023 Data Breach Investigations Report”, 2023, Available: https://enterprise.verizon.com/resources/reports/dbir

[6] D. Kotz, C. A. Gunter, S. Kumar and J. P. Weiner, "Privacy and Security in Mobile Health: A Research Agenda," in Computer, vol. 49, no. 6, pp. 22-30, June 2016, doi: 10.1109/MC.2016.185.

[7] A. J. Burns, M. Eric Johnson, and Peter Honeyman, “A brief chronology of medical device security”, Commun. ACM 59, 10, October 2016, 66–72. Available: https://doi.org/10.1145/2890488

[8] Angela Coulter, Graham Kramer, Tim Warren, Chris Salisbury, "Building the House of Care for people with long-term conditions: the foundation of the House of Care framework", 2016, Available: https://doi.org/10.3399/bjgp16X684745

[9] Microsoft, "Windows XP", Available: https://learn.microsoft.com/en-us/lifecycle/products/windows-xp

[10] LUXSCI, "Why Are Hackers Targeting Your Medical Records?", 2017, Available: https://luxsci.com/blog/hackers-targeting-medical-records.html

[11] WADA, "Cyber Security Update: WADA’s Incident Response", 2016, Available: https://www.wada-ama.org/en/news/cyber-security-update-wadas-incident-response

[12] Kim Sengupta, "Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images", 2017, Available: https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html

[13] OAIC, "DonateBlood.com.au data breach (Australian Red Cross Blood Service)", 2017, Available: https://www.oaic.gov.au/__data/assets/pdf_file/0022/2839/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf

[14] Ramo Sendelj, Ivana Ognjanovic, "Cybersecurity Challenges in Healthcare", 2022, Available: https://ebooks.iospress.nl/doi/10.3233/SHTI220951

[15] HHS, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients", 2023, https://405d.hhs.gov/Documents/HICP-Main-508.pdf

[16] Filipa Capelão, Hugo Barbosa, "Cybersecurity in Health-care: Risk Analysis in Health Institution in Portugal", 2018, Available: https://www.ijrdt.org/full_paper/31565/19/CybersecurityinHealthcareRiskAnalysisinHealthInstitution-in-Portugal

[17] Dr. James Angle, "Ransomware in the Healthcare Cloud", 2021, Available: https://cloudsecurityalliance.org/artifacts/ransomware-in-the-healthcare-industry/

[18] Steve G. Langer, "Cyber-Security Issues in Healthcare Information Technology", J Digit Imaging 30, 117–125, 2017, Available: https://doi.org/10.1007/s10278-016-9913-x

[19] Meenakshi Mittal, Krishan Kumar & Sunny Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review", Soft Comput 27, 13039–13075, 2023, Available: https://doi.org/10.1007/s00500-021-06608-1

[20] HHS, "Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations", 2023, Available: https://405d.hhs.gov/Documents/tech-vol2-508.pdf

[21] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819

[22] Mateus-Coelho, Nuno Ricardo, et al. "POSMASWEB: Paranoid Operating System Methodology for Anonymous and Secure Web Browsing." Handbook of Research on Cyber Crime and Information Privacy, edited by Maria Manuela Cruz-Cunha and Nuno Mateus-Coelho, IGI Global, 2021, pp. 466-497. https://doi.org/10.4018/978-1-7998-5728-0.ch023